JOURNAL OF COMBINATORIAL THEORY, Series B 28, 18–25 (1980)

Symmetries of Directed Graphs and the Chinese Remainder Theorem

STEPHANE FOLDES

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Communicated by the Editors

Received March 29, 1977

It is shown that a permutation group on a finite set is the automorphism group of some directed graph if and only if a generalized Chinese remainder theorem holds for the family of stabilizers. This result can be applied to examine some special permutation groups, including the general linear groups of finite vector spaces.

1. INTRODUCTION AND TERMINOLOGY

All sets, families, and groups in the first two sections are assumed to be finite. The cardinality of a set V is denoted by $|V|$. Permutations act on the left. A *permutation group* G on V is any subgroup of S_V, the group of all permutations of V. For $x \in V$, the *stabilizer* of x in G is $G_x = \{f \in G \mid f(x) = x\}$. A central role will be played by the *family* $(G_x)_{x \in V}$ *of stabilizers*. We recall that an *orbit* of G is a minimal nonempty $S \subseteq V$ such that for every $f \in G$, $f(S) = S$, and that G is *regular* if V is an orbit and the stabilizers are trivial.

A *directed graph* D is an ordered triple $D = (V, A, w)$, where $V = V(D)$ and $A = A(D)$ are arbitrary sets, and $w = w_D$ is a mapping from A to the cartesian square V^2. The elements of V and A are called, respectively, *vertices* and *arcs*, and w is called the *incidence function*. If $w(a) = (x, y)$, then a is said to be an arc *from* x *to* y. The arc a is a *loop* if $w(a) = (x, x)$. We deviate from the usual terminology by calling a directed graph D *simple* if $A(D)$ is a subset of V^2 and the incidence function is the identity. Thus, simple directed graphs can have loops. To define a simple directed graph, it suffices to specify its vertex set and its arcs.

An *automorphism* of a directed graph D is a permutation f of $V(D)$ such that for every $x, y \in V(D)$ the number of arcs from x to y equals the number of arcs from $f(x)$ to $f(y)$. The set of all automorphisms is a permutation group on $V(D)$, denoted Aut D. It follows from the well-known theorem of Frucht

0095-8956/80/010018–08$02.00/0

[6] that every group is isomorphic to the automorphism group of some directed graph. However, not every permutation group on a set V is the automorphism group of some directed graph on vertex set V. The simplest counterexamples are the doubly transitive proper subgroups of S_V, in particular, the alternating groups A_V, $|V| \geqslant 4$.

PROPOSITION 1.1. *Let V be any set. For every permutation group G on V the following two conditions are equivalent*:

(i) *G is the automorphism group of some directed graph D on V;*

(ii) *$G = \bigcap_{i \in I} \operatorname{Aut} D_i$ for some family $(D_i)_{i \in I}$ of simple directed graphs on V.*

Proof. (i) $\Rightarrow$ (ii). For every nonnegative integer k let D_k be the simple directed graph with vertex set V, defined by

$$A(D_k) = \{(x, y) \in V^2 \mid |w_D^{-1}(x, y)| = k\}.$$

Clearly there is some integer n with the property that $A(D_k)$ is empty if $k \geqslant n$. We have

$$\operatorname{Aut} D = \bigcap_{k<n} \operatorname{Aut} D_k .$$

(ii) $\Rightarrow$ (i). Let f be an injective function associating with every subset S of I some nonnegative integer $f(S)$. Let D be a directed graph with vertex set V and such that for every $x, y \in V$, the number of arcs from x to y is

$$f(\{i \in I \mid (x, y) \in A(D_i)\}).$$

The automorphism group of D is G. ∎

COROLLARY 1.2. *Let V be any set. The set of subgroups of S_V that are automorphism groups of directed graphs is closed under intersection.*

The above corollary does not hold if "directed graphs" is replaced by "simple directed graphs." Indeed, let V be any set having at least four elements. Let D be a directed graph on V consisting of a component represented in Fig. 1 and $|V| - 4$ isolated vertices. It is easy to see that $\operatorname{Aut} D = \operatorname{Aut} D_1 \cap \operatorname{Aut} D_2$, where D_1 and D_2 are simple directed graphs. However, there exists no simple directed graph D' on V with $\operatorname{Aut} D' = \operatorname{Aut} D$.

It can be seen without difficulty that for every directed graph D there is a loopless directed graph D' on the same vertex set, and such that $\operatorname{Aut} D' = \operatorname{Aut} D$.

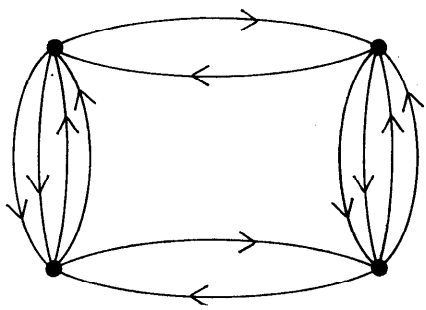

FIGURE 1

2. CHARACTERIZATION OF AUTOMORPHISM GROUPS OF DIRECTED GRAPHS

Let S and S' be subsets of an abstract group G. We define $S^{-1} = \{x^{-1} \mid x \in S\}$ and $SS' = \{xy \mid x \in S, y \in S'\}$. If x and y are elements of G such that $x^{-1}y \in S$, then we say that x is *congruent to* y modulo S and we write

$$x \equiv y \bmod S.$$

This congruence relation is reflexive if and only if the unit element of G belongs to S, symmetric if and only if $S^{-1} = S$. It is an equivalence relation if and only if S is a subgroup of G. The left regularity law

$$\forall x, y, z \in G \qquad (x \equiv y \bmod S \Leftrightarrow zx \equiv zy \bmod S)$$

is always satisfied, while the right regularity law

$$\forall x, y, z \in G \qquad (x \equiv y \bmod S \Leftrightarrow xz \equiv yz \bmod S)$$

holds if and only if S is stable by every inner automorphism of G. In particular, we have a regular group congruence if and only if S is a normal subgroup of G. The following is an obvious generalization of the classical Chinese remainder theorem.

PROPOSITION 2.1. *Let S_1 and S_2 be subsets of a group G such that $S_1^{-1} = S_1$ and $S_2^{-1} = S_2$. Let x_1 and x_2 be arbitrary elements of G. Then the following two conditions are equivalent*:

(i) *There exists an $x \in G$ satisfying the two simultaneous congruences*

$$\begin{aligned} x &\equiv x_1 \bmod S_1, \\ x &\equiv x_2 \bmod S_2; \end{aligned} \tag{1}$$

(ii) $x_1 \equiv x_2 \bmod S_1S_2$.

Proof. If x satisfies (1), then $x_1^{-1}x_2 = (x_1^{-1}x)(x^{-1}x_2)$ belongs to $S_1^{-1}S_2 = S_1S_2$. Conversely, assume that $x_1^{-1}x_2 = s_1s_2$, where $s_1 \in S_1$, $s_2 \in S_2$. Then

$$x = x_1s_1 = x_2s_2^{-1}$$

is a solution of the system (1). ∎

COROLLARY 2.2. *Let $(S_i)_{i\in I}$ be a family of subsets of a group G such that for every $i \in I$, $S_i^{-1} = S_i$. Let $(x_i)_{i\in I}$ be a family of elements of G indexed by the same set I. If*

$$\exists\, x \in G\ \forall\, i \in I \qquad (x \equiv x_i \bmod S_i), \tag{2}$$

then

$$\forall\, i, j \in I \qquad (x_i \equiv x_j \bmod S_iS_j). \tag{3}$$

We say that the *Chinese remainder theorem holds* for a family $(S_i)_{i\in I}$ of subsets of a group G if for every family $(x_i)_{i\in I}$ of elements of G, condition (2) is equivalent to (3). We shall be interested in the case where all the S_i are subgroups of G. But even then, the products S_iS_j need not be subgroups.

PROPOSITION 2.3. *Let $(G_i)_{i\in I}$ be a family of permutation groups on a set V. If for every i, the Chinese remainder theorem holds for the family of stabilizers of G_i, then it also holds for the family of stabilizers of the intersection $\bigcap_i G_i$.*

Proof. Let $G = \bigcap_i G_i$ and for every $x \in V$ let f_x be an element of G. Assume that

$$\forall x, y \in V \qquad (f_x \equiv f_y \bmod G_xG_y).$$

For every $i \in I$, we have a fortiori

$$\forall x, y \in V \qquad (f_x \equiv f_y \bmod (G_i)_x(G_i)_y),$$

and applying the Chinese remainder theorem we can find a solution $f_i \in G_i$ to the system

$$\forall x \in V \qquad (f_i \equiv f_x \bmod (G_i)_x).$$

Each f_i, $i \in I$, is obviously a solution of the system

$$\forall x \in V \qquad (f_i \equiv f_x \bmod (S_V)_x).$$

But it is easy to see that this sytem cannot have more than one solution in S_V. This proves that all the f_i, $i \in I$, are the same permutation f. Also we have $f \in \bigcap_i G_i = G$, proving that

$$\forall x \in V \qquad (f \equiv f_x \bmod G_x). \quad ∎$$

PROPOSITION 2.4. *A permutation group G on a set V is the automorphism group of some directed graph on vertex set V if and only if the Chinese remainder theorem holds for the family $(G_x)_{x\in V}$ of stabilizers.*

Proof. If G is the automorphism group of some directed graph, then according to Proposition 1.1 there exists a family $(D_i)_{i\in I}$ of simple directed graphs on V such that $G = \bigcap_i \mathrm{Aut}\, D_i$. Therefore, in view of Proposition 2.3 it will suffice to show that the Chinese remainder theorem holds for the family of stabilizers of the group of any simple directed graph D. Let $(f_x)_{x\in V}$ be a family of automorphisms of D such that

$$\forall x, y \in V \qquad (f_x \equiv f_y \bmod (\mathrm{Aut}\, D)_x(\mathrm{Aut}\, D)_y).$$

Consider the mapping f from V to itself defined by $f(x) = f_x(x)$ for every $x \in V$. First, we show that f is a permutation. Indeed, if $f_x(x) = f_y(y)$, then $f_x^{-1}f_y(y) = x$. By assumption, $f_x^{-1}f_y = g_x g_y$ for some $g_x \in \mathrm{Aut}\, D)_x$, $g_y \in (\mathrm{Aut}\, D)_y$. But then

$$x = f_x^{-1}f_y(y) = g_x g_y(y) = g_x(y),$$

implying that $x = y$. This proves that f is injective. Since V is finite, f must be bijective. Next, let (x, y) be an arc of D. Let $h = f_x g_x = f_y g_y^{-1}$, where $g_x \in (\mathrm{Aut}\, D)_x$, $g_y \in (\mathrm{Aut}\, D)_y$. Since h is an automorphism of D, $(f(x), f(y)) = (f_x(x), f_y(y)) = (h(x), h(y))$ is an arc of D. This shows that f is an automorphism of D, and it is obviously a solution of the congruence system

$$\forall x \in V \qquad (f \equiv f_x \bmod (\mathrm{Aut}\, D)_x).$$

This proves that the Chinese remainder theorem holds for the family of stabilizers.

Conversely, assume that the Chinese remainder theorem holds for the family of stabilizers of the permutation group G. According to Proposition 1.1, to prove that G is the automorphism group of some directed graph on V, it will suffice to show that $G = \bigcap_{i\in I} \mathrm{Aut}\, D_i$ for some family $(D_i)_{i\in I}$ of simple directed graphs on V. For every $x \in V$ and every orbit C of G_x, we define a simple directed graph $D_{x,C}$ with vertex set V by

$$A(D_{x,C}) = \bigcup_{g\in G} \{(g(x), y) \mid y \in g(C)\}. \tag{4}$$

Every $h \in G$ is an automorphism of every $D_{x,C}$, so that $G \subseteq \bigcap_{x,C} \mathrm{Aut}\, D_{x,C}$, where the intersection is taken over all $x \in V$ and all orbits C of G_x. We shall show that for every $f \in \bigcap_{x,C} \mathrm{Aut}\, D_{x,C}$ there is a family $(f_x)_{x\in V}$ of elements of G such that

$$\forall x \in V \qquad (f \equiv f_x \bmod G_x). \tag{5}$$

This would imply $f \in G$ for every such f, and the equality $G = \bigcap_{x,C} \mathrm{Aut}\, D_{x,C}$ would follow. To prove our claim, assume that $f \in \bigcap_{x,C} \mathrm{Aut}\, D_{x,C}$. Observe that for every $x \in V$ the orbit of G containing x is

$$\{ y \in V \mid (y, y) \in A(D_{x,\{x\}}) \}.$$

Since $f \in \mathrm{Aut}\, D_{x,\{x\}}$ for every $x \in V$, it follows that every cycle of f is contained in some orbit of G, i.e., for every $x \in V$ there is some $f_x \in G$ with $f_x(x) = f(x)$. Obviously

$$\forall x \in V \qquad (f \equiv f_x \bmod (S_V)_x). \tag{6}$$

If we can show that

$$\forall x, y \in V \qquad (f_x \equiv f_y \bmod G_x G_y), \tag{7}$$

then applying the Chinese remainder theorem we can find a solution $g \in G$ to the congruence system

$$\forall x \in V \qquad (g \equiv f_x \bmod G_x). \tag{8}$$

A fortiori g will be a solution of the system

$$\forall x \in V \qquad (g \equiv f_x \bmod (S_V)_x).$$

But this system can have only one solution. Comparing with (6) yields $f = g$, and (8) becomes (5). To prove (7), let us fix $x, y \in V$. Let C be the orbit of G_x containing y. Since $f \in \mathrm{Aut}\, D_{x,C}$ and (x, y) is an arc of $D_{x,C}$, $(f(x), f(y)) = (f_x(x), f_y(y))$ is also an arc of $D_{x,C}$. Applying $f_x^{-1} \in G \subseteq \mathrm{Aut}\, D_{x,C}$ we get $(x, f_x^{-1} f_y(y)) \in A(D_{x,C})$. By the definition (4) of $D_{x,C}$ this means that for some $g_x \in G_x$, $f_x^{-1} f_y(y) = g_x(y)$, i.e., $g_x^{-1} f_x^{-1} f_y \in G_y$. The congruence

$$f_x \equiv f_y \bmod G_x G_y$$

immediately follows. ∎

Remark. The underlying principle of the above proof is a generalization of the Cayley color graph construction [4, 12]. Similar methods were also used by Jonsson [9, 10] and Plonka [13] in the description of automorphism groups of universal algebras.

COROLLARY 2.5. *Every permutation group generated by a single permutation is the automorphism group of some directed graph.*

Proof. Camion *et al.* [3] have shown that the Chinese remainder theorem holds for every family of normal subgroups of a group G that generate a distributive sublattice of the lattice of all subgroups of G. If G is generated by a single element, then every subgroup of G is normal and the lattice of subgroups is distributive [11]. ∎

COROLLARY 2.6. *Every permutation group having at most two distinct stabilizers is the automorphism group of some directed graph.*

Proof. According to Proposition 2.1 the Chinese remainder theorem holds for any two subgroups of a group. ∎

COROLLARY 2.7. *Every permutation group G having at least one trivial stabilizer G_x is the automorphism group of some directed graph.*

Proof. Let G be a permutation group on a set V, and let $x \in V$ such that G_x is trivial. We show that the Chinese remainder theorem holds for the family of stabilizers of G. Let $(f_y)_{y \in V}$ be a family of elements of G such that

$$\forall y, z \in V \qquad (f_y \equiv f_z \bmod G_y G_z).$$

In particular, we have, since G_x is trivial,

$$\forall y \in V \qquad (f_x \equiv f_y \bmod G_y). \quad ∎$$

COROLLARY 2.8. *If at least one stabilizer G_x of a permutation group G is trivial, then every subgroup of G is the automorphism group of some directed graph.*

COROLLARY 2.9. *Every regular permutation group is the automorphism group of some directed graph.*

According to Proposition 1.1 and Corollary 2.9, every regular permutation group G is of the form $G = \bigcap_i \operatorname{Aut} D_i$, where the D_i are simple directed graphs. If we think of the different D_i as represented in the same diagram, the arcs of each D_i being distinguished from the other arcs by the assignment of some "color i," then we have essentially a redundant Cayley color graph.

Let V be an n-dimensional vector space over a q-element field F. Using Proposition 2.4 we can determine when the group $GL(n, q)$ of invertible linear transformations of V is the automorphism group of some directed graph on V.

PROPOSITION 2.10 [5]. *$GL(n, q)$ is the automorphism group of some directed graph on V if and only if $n = 1$ or $n = q = 2$.*

3. Generalizations to the Infinite Case

All concepts defined in the preceding sections also apply if we make no restriction to finite cardinalities. Propositions 1.1, 2.1, 2.3, and 2.10 and Corollaries 1.2, 2.2, 2.6, 2.7, 2.8, and 2.9 are also valid in the infinite case. The infinite version of Proposition 2.4 is generally not true: It can be shown that if V is an infinite set, then the Chinese remainder theorem fails to hold for the family of stabilizers of the full symmetric group S_V, despite the fact that the latter is the automorphism group of the arcless directed graph on V. However, Proposition 2.4 holds for those permutation groups G on an infinite set, all stabilizers of which are normal subgroups of G. In particular, this is the case if G is abelian (see [5]). Corollary 2.5 should be replaced by the following if infinite sets are allowed.

Proposition 3.1 [5]. *A permutation group G generated by a single permutation is the automorphism group of some directed graph if and only if G is of finite order or it has an infinite orbit.*

References

1. N. L. Biggs, "Finite groups of automorphisms," Cambridge Univ. Press, London, 1971.
2. J. A. Bondy and U. S. R. Murty, "Graph Theory with Applications," Macmillan, New York, 1976.
3. P. Camion, C. S. Levy, and H. B. Mann, Linear equations over a commutative ring, *J. Algebra* **18** (1971), 432–446.
4. A. Cayley, The theory of groups, *Proc. London Math. Soc.* **9** (1978), 126–133.
5. S. Foldes, "Symmetries," Ph.D. thesis, University of Waterloo, Waterloo, Canada, 1977.
6. R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Compositio Math.* **6** (1939), 239–250.
7. F. Harary and E. Palmer, The groups of the small digraphs, *J. Indian Statist. Assoc.* **4** (1966), 155–169.
8. R. L. Hemminger, On the group of a directed graph, *Canad. J. Math.* **18** (1966), 211–220.
9. B. Jonsson, Algebraic structures with prescribed automorphism groups, *Colloq. Math.* **19** (1968), 1–4.
10. B. Jonsson, "Topics in Universal Algebra," Lecture Notes in Mathematics No. 250, Springer-Verlag, New York, 1972.
11. O. Ore, Structures and group theory, II, *Duke Math. J.* **4** (1938), 247–269.
12. O. Ore, "Graph Theory," AMS Colloquium Publ., Amer. Math. Soc., Providence, R.I., 1962.
13. E. Plonka, A problem of B. Jonsson concerning automorphisms of a general algebra, *Colloq. Math.* **19** (1968), 5–8.
14. H. Wielandt, "Finite Permutation Groups," Academic Press, New York, 1964.